Recorded Future Alerts - QRadar Installation Guide v1.0.1

Application Description

Recorded Future is continuously harvesting data from Open, Deep, and Dark Web sources in real-time including Social media, Forums, Blogs, IRC channels, Paste sites, email groups, onion sites via TOR, and more through a range of collection mechanisms. Thousands of sources are added to our index for customers each week and are currently mining and cross-correlating data from over 750,000+ sources in seven languages with a patented Temporal Analytics™ Engine.

The Recorded Future application for IBM QRadar enables:

- Delivery of Recorded Future Alert details consumed in IBM QRadar as events via custom Recorded Future log sources.
- Triaging Recorded Future Alerts and Playbook Alerts with the full alert details context directly in the IBM QRadar product.
- Review trending Inteligence Goals Library (IGL) data.

- Ability to document historial credential leaks.

The Recorded Future Alerts application for IBM QRadar enables better alerts triaging by adding relevant and comprehensive context.

System Requirements

- IBM QRadar version 7.4.1 Fix Pack 2 or higher
- IBM QRadar Authorized Services Token (Admin)
- Recorded Future Connect API Token
- TCP Port 514 open from QRadar server where the application is running to the syslog destination
- Recorded Future account for accessing content when pivoting outside IBM QRadar to the Recorded Future platform

Installation

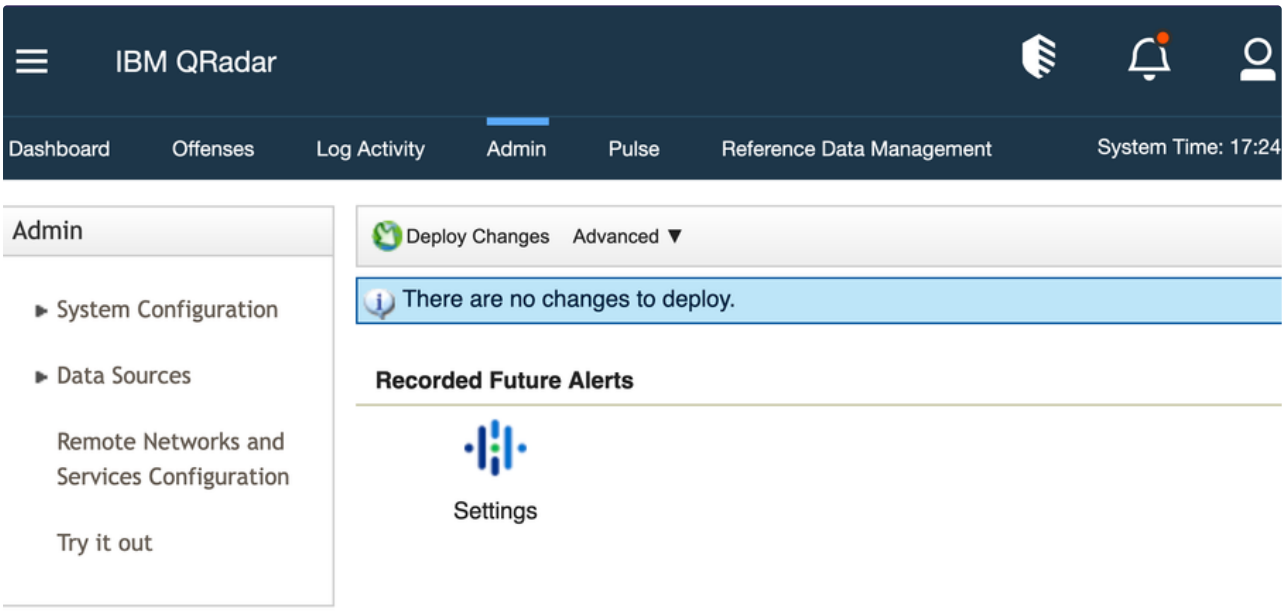
The preferred installation method for Recorded Future Alerts application is by uploading the application zip file via Extension Management.

Configuration

Once the Recorded Future Alerts application is installed, the “Settings” icon should be already visible under the “Admin” tab from IBM QRadar in the “Plug-ins” sections.

Before configuring the application itself, please complete these steps in the following order:

1. Creating an authorized service token
2. Importing Pulse dashboards
3. Custom Rules
4. Increase Max TCP Payload Length
5. Recorded Future Alerts configuration



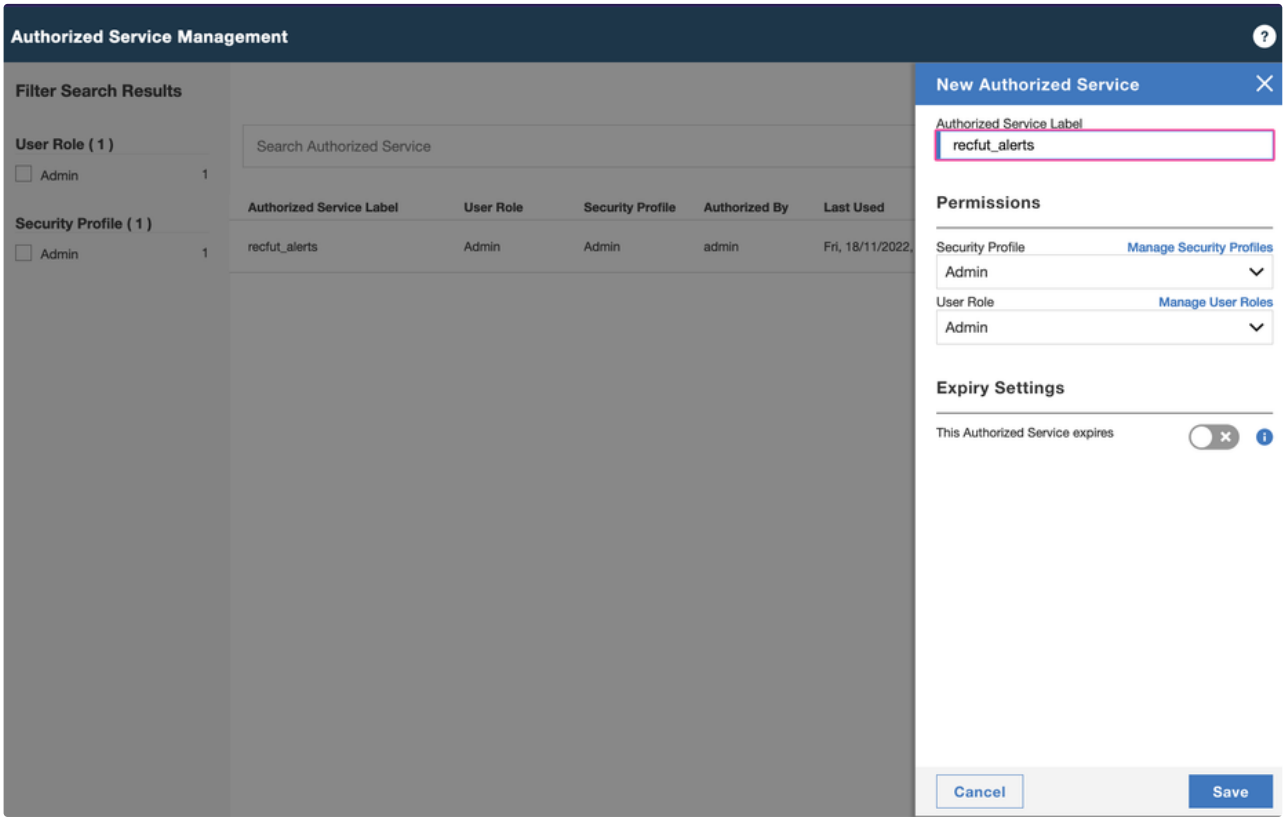
Creating an authorized service token

The Recorded Future Alerts application requires an IBM QRadar Authorized Service Token (AST) to operate.

Note: QRoC customers get their AST from the "self Serve App" See: Authorized service tokens

Please use the following steps to create such a Token that you can later use in the application configuration window:

1. Click on the **Admin** tab
2. Click **Authorized Services**
3. Click **+Add**
4. In the **Authorized Service Label**, type a name for the authorized service
5. From the **Security Profile** list, select **Admin**
6. From the **User Role** list, select **Admin**
7. Set the desired token expiry period



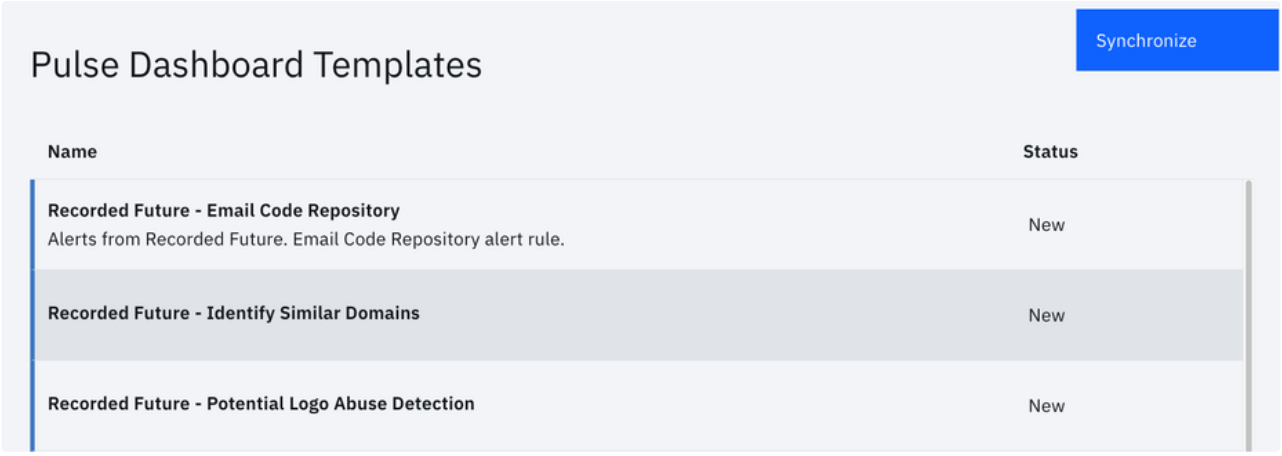
8. Click **Save**

Once the service is created, the newly created **Authentication Token** is displayed and can be copied. Please note that, the authorized service token cannot be made visible after you close the **Authorized Service Created Successfull**y dialog. Copy the token to a secure location before you close the dialog. Link for reference: Adding an authorized service

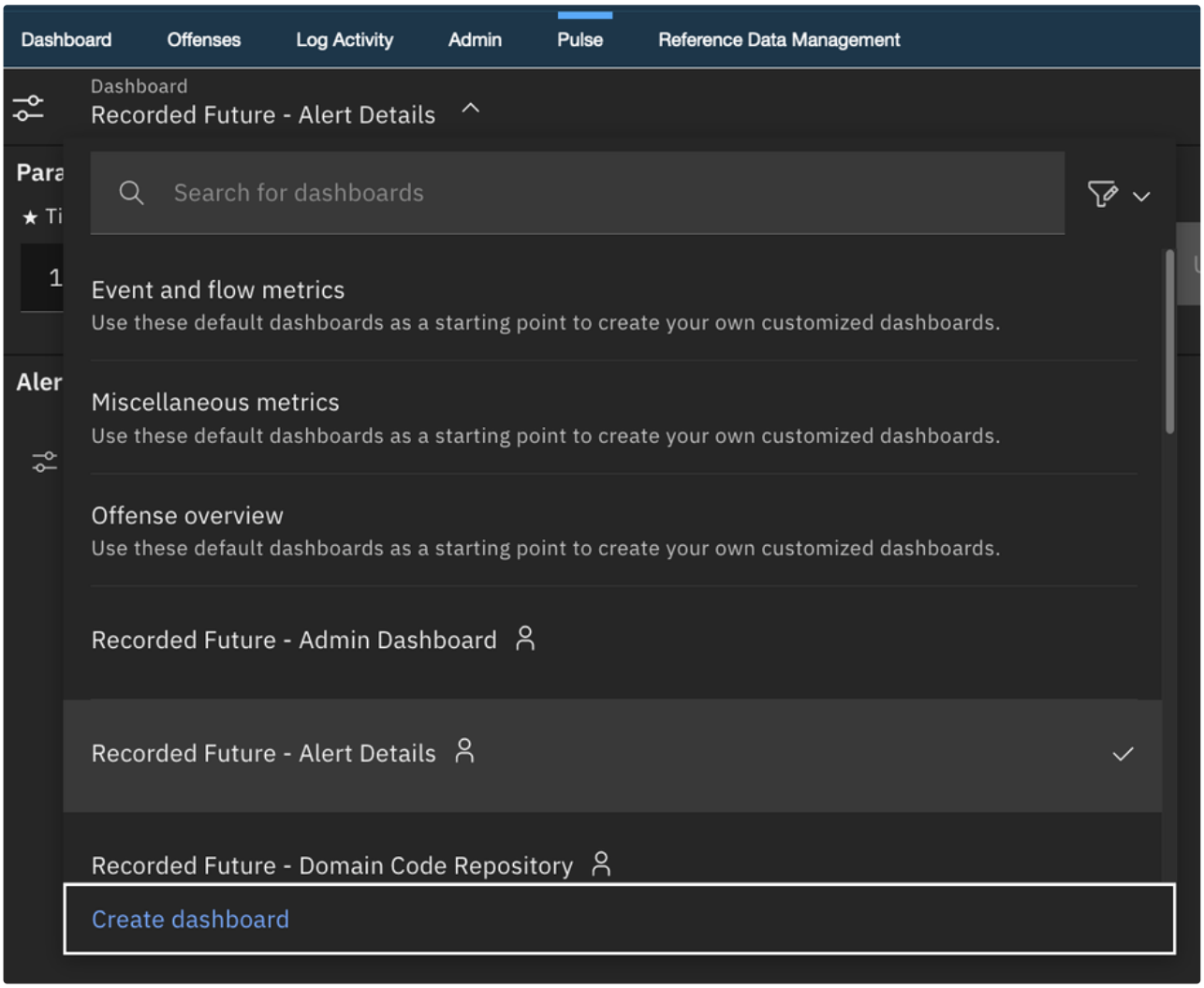
Importing Pulse dashboards

The application comes with a set of dashboards which allow to quickly visualise and effectively triage Recorded Future alerts & playbook alerts in the IBM QRadar Pulse application. To install the dashboards, please follow the steps detailed below:

1. Click on the **Admin** tab
2. Click **Pulse - Dashboard**
3. Click **Synchronize**



4. Click on the **Pulse** tab
5. Click on the **Dashboard** dropdown
6. Click **Create Dashboard**



7. Click **Manage templates**
8. Click **Install** for each **Recorded Future** named dashboard

Custom Rules

The application comes with a set IBM QRadar Offense Rules to enable offense generation. These rules can be found in the **Recorded Future Alerts** group.

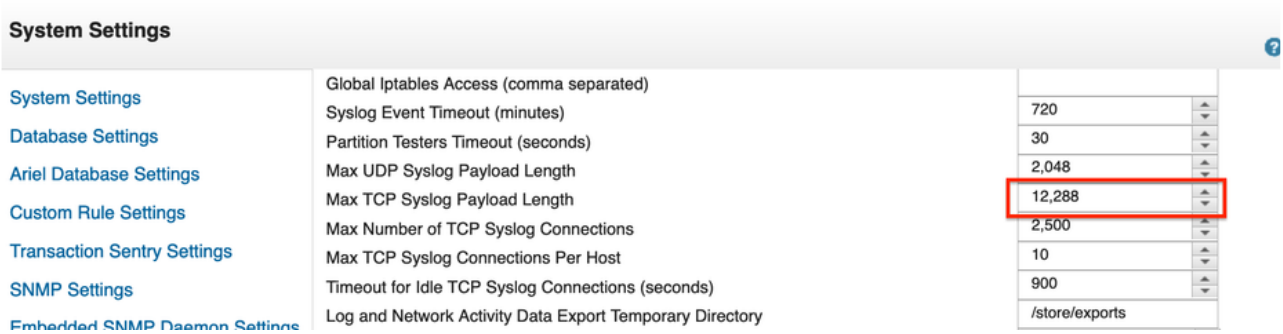
By default these rules are enabled and will generate an offense per Recorded Future alert.

Non parsing alerts will not generate offenses.

Increase Max TCP Syslog Payload Length

Because alerts and playbook alerts are sent via syslog and some of the alert payloads can be rather large, this can easily top the QRadar default settings for the Max TCP Syslog Payload Length. This will result in some Recorded Future alert payloads being truncated and not parsing correctly. To avoid this issue from happening, follow the steps outlined below:

1. Click on the **Admin** tab
2. Click **System Settings**
3. Click **Advanced**
4. In the **Max TCP Syslog Payload Length** field, type **12288**

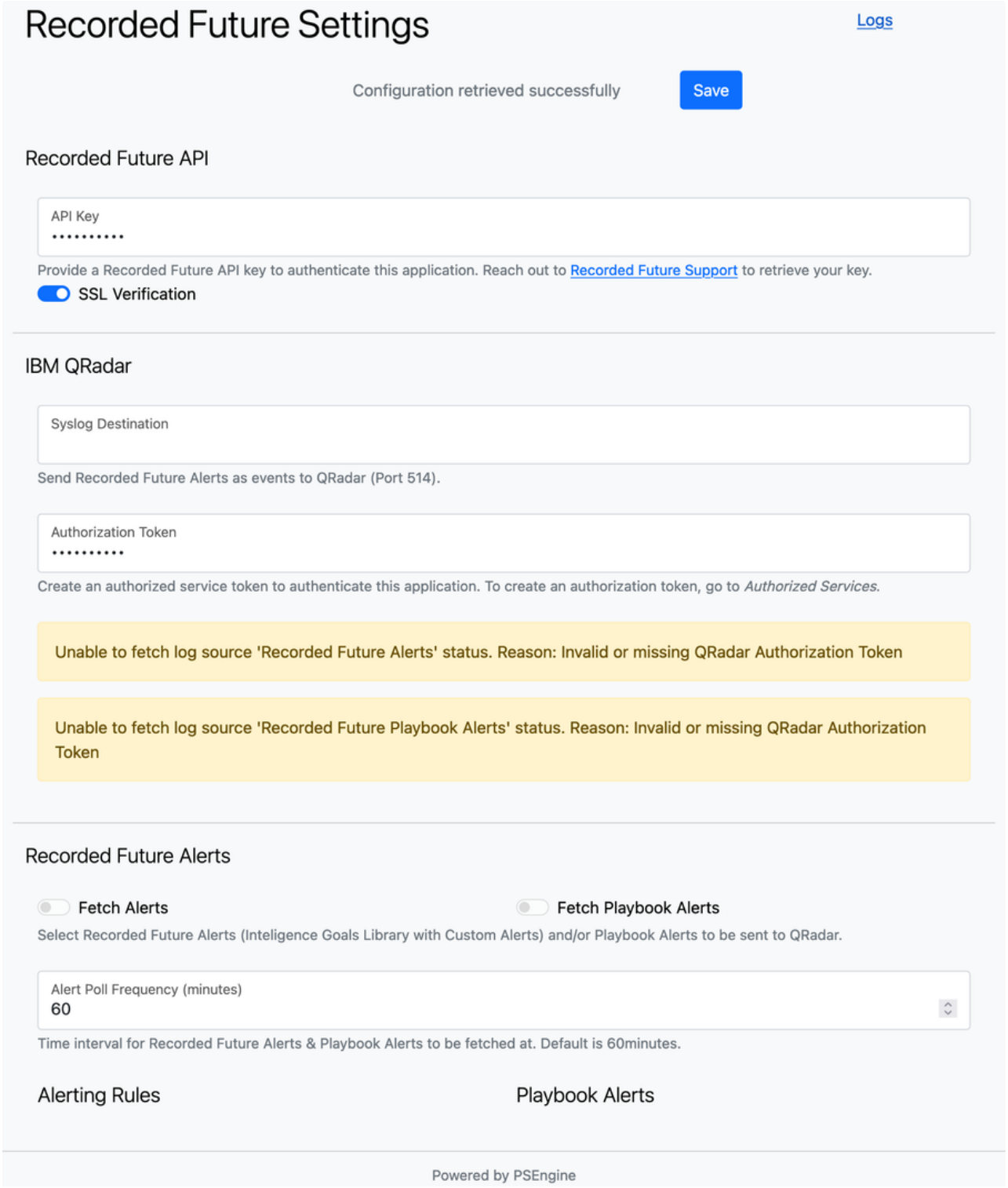


5. Click **Save**
6. The changes made will require a **Full Deploy**, click on the **Admin** tab
7. From the **Advanced** list, click **Deploy Full Configuration**
8. After services restart, the QRadar deployment is updated to allow TCP packets that are up to **12288** bytes without truncation

More information about the topic QRadar: TCP and UDP Syslog Maximum Payload Message Length for QRadar Appliances

Recorded Future Alerts configuration

The configuration page for the Recorded Future Alerts application can be found in the **Admin** tab within the **Plug-ins** section. Once opened the configuration page will enable configuration of the following parameters:



Logs

- *Logs* - links to application logs

Recorded Future API

- *API Key* - Recorded Future API Token
- *SSL verification switch* - Allows to disable SSL certificates verification when reaching out to the Recorded Future API

IBM QRadar

- *Syslog Destination* - IP/Hostname of a QRadar syslog destination which the Recorded Future Alerts application uses to send alerts as events via syslog on port 514.
- *Authorization Token* - IBM QRadar Authorized Service Security Token created in the previous steps

Recorded Future Alerts

- *Fetch Alerts switch* - when disabled Recorded Future Alerts will not be downloaded
- *Fetch Playbook Alerts switch* - when disabled Recorded Future Playbook Alerts will not be downloaded
- *Alert Poll Frequency* - controls how often the alerts & alert updates (applicable to Playbook Alerts) be ingested. Defaults to 60 minutes, lowest supported interval is 15 minutes.
- *Alerting Rules list* - selected alerting rules will be ingested
- *Playbook Alerts list* - selected playbook alerts will be ingested


List of alert rules to select will only be available once the configuration has a valid Recorded Future API Key saved.

Application Functionality

Recorded Future Alerts application's functionality is underpinned by the Recorded Future API, which is the repository from which QRadar retrieves the Recorded Future Alerts and Playbook Alerts. The app fetches alert details and provides them to QRadar via two log sources **Recorded Future Alerts** and **Recorded Future Playbook Alerts**. This makes the alerts context ready for triaging and advanced correlation in IBM QRadar.

Triage alerts

Ingested alerts become searchable with the help of AQL queries and a set of Pulse dashboards detailed later in this document.

Triage using AQL

The query below returns all ingested Recorded Future Alerts from the past 3 days.

```
SELECT
    "Alert ID",
    "Alert Title" AS "Alert Title",
    DATEFORMAT("Alert Triggered Time", 'yyyy-MM-dd hh:mm:ss')  AS 'Triggered Time',
    "Alert URL" AS 'Alert URL',
    logsourcename(logsourceid) AS log_source_name
FROM events
WHERE (
    log_source_name = 'Recorded Future Alerts'
 )
GROUP BY "Alert ID"
ORDER BY "Triggered Time" DESC  last 3 Days
```

The query below returns all ingested Recorded Future Playbook Alerts from the past 3 days.

```
SELECT
    "Entity Name" AS "Entity Name",
    "Alert ID",
    DATEFORMAT("Alert Triggered Time", 'yyyy-MM-dd hh:mm:ss')  AS 'Triggered Time',
    "Alert URL" AS 'Alert URL',
    logsourcename(logsourceid) AS log_source_name
FROM events
WHERE (
    log_source_name = 'Recorded Future Playbook Alerts'
 )
```

```
GROUP BY "Alert ID"
ORDER BY "Triggered Time" DESC  last 3 Days
```

The query below returns all email addresses and passwords that have been leaked with the market name where they are sold.

```
SELECT
    "Email Leaked" AS "Leaked Email",
    "Leaked Password",
    "Alert Source Name" AS "Source Name",
    DATEFORMAT("Alert Triggered Time", 'yyyy-MM-dd hh:mm:ss')  AS 'Triggered Time',
    logsourcename(logsourceid) AS log_source_name
FROM events
WHERE (
    "Alert Rule Name"='Leaked Credential Monitoring' AND
    log_source_name = 'Recorded Future Alerts'
)
ORDER BY "Triggered Time" DESC last 3 DAYS
```

The query below returns all the similar domains (example typosquats) that have been seen in the last 3 days.

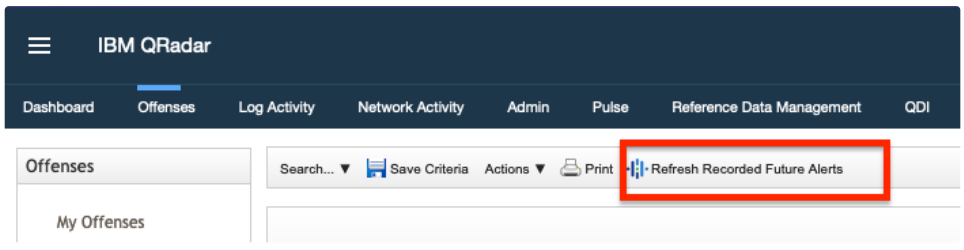
```
SELECT
    "Alert Source Name" AS "Repo Name",
    "Similar Domain" AS "Domain",
    DATEFORMAT("Alert Triggered Time", 'yyyy-MM-dd hh:mm:ss')  AS "Triggered Time",
    logsourcename(logsourceid) AS log_source_name
FROM events
WHERE (
    "Alert Rule Name"='Identify Similar Domains' AND
    log_source_name = 'Recorded Future Alerts'
)
ORDER BY "Triggered Time" DESC last 3 DAYS
```

The query below returns a list of target domains that have been triggered by the domain abuse playbook alert in the last 3 days.

```
SELECT
    "Entity Name" AS "Domain",
    "Targets List" AS "Target",
    DATEFORMAT("Alert Triggered Time", 'yyyy-MM-dd hh:mm:ss')  AS 'Triggered Time',
    logsourcename(logsourceid) AS log_source_name
FROM events
WHERE (
    "Alert Rule Name" = 'Domain Abuse' AND
    log_source_name = 'Recorded Future Playbook Alerts'
 )
ORDER BY "Triggered Time" DESC last 3 DAYS
```

Fetch alerts

The users can trigger an alert poll ahead of schedule from the **Offenses** tab.



Please note in may take some time before new alerts become searchable in QRadar as the system can take time to process the events. The exact amount of time depends on the size and load of the QRadar deployment.

Pulse dashboards

Some tables in the dashboards will not present data straight away. It is require that you select the row (alert) that you are interested into to get the details in the subsequent tables.

Also note that for more details all the dashboards link back to the Recorded Future App. A valid Recorded Future account is needed to see those details.

Below are reported all the actions that you can perform without having access to the Recorded Future App.

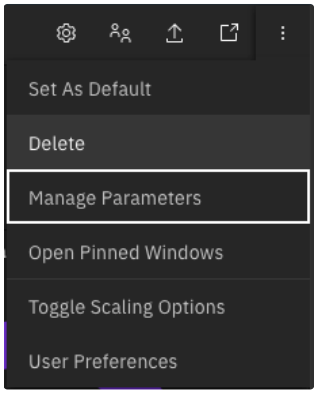
Organisation Filter

Every user will have a filter called “Organisation” in each dashboard. This is used to filter for specific Recorded Future Alerts based on the Organisation in which the alert triggered. To select an organisation, just enter a part of the organisation name and click Update

If you want to see all the alerts from all the organisations, enter a dot (`.`)

If you do not have Multi-Org enabled in the Recorded Future Portal, just configure the Organisation filter, with the dot (`.`) character:

- In the top right side click on the three dots
- Click on **Manage Parameters**



- Search for “Organisation”
- Set “Default value” as `.`
- Click **Save**

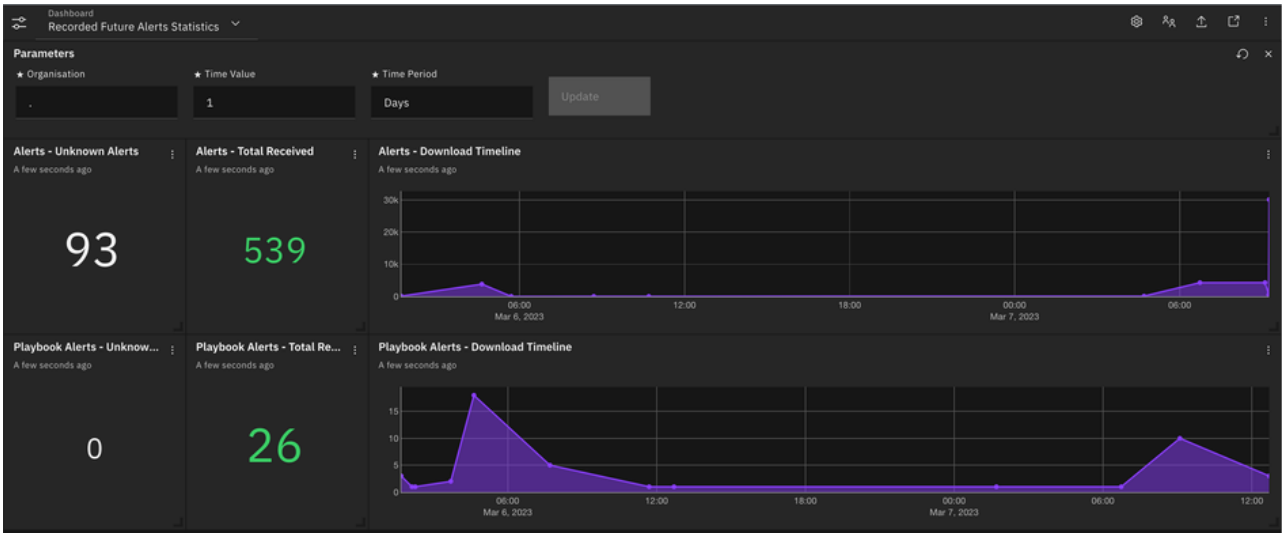
Alert Rules List

Below is the list of Alert Rules, both legacy and playbook alerts, that you will find out of the box.

- Domain Abuse
- Domain Code Repository
- Email on Code Repository
- Identify Similar Domains
- Leaked Credential Monitoring
- Leaked Email Monitoring
- My domains on Dark Web and closed Sources
- New Critical or Pre NVD Watch List Vulnerabilities (Global)
- New Critical or Pre NVD Watch List Vulnerabilities (Tech Stack)
- Potential Logo Abuse Detection

Recorded Future Alerts Statistics

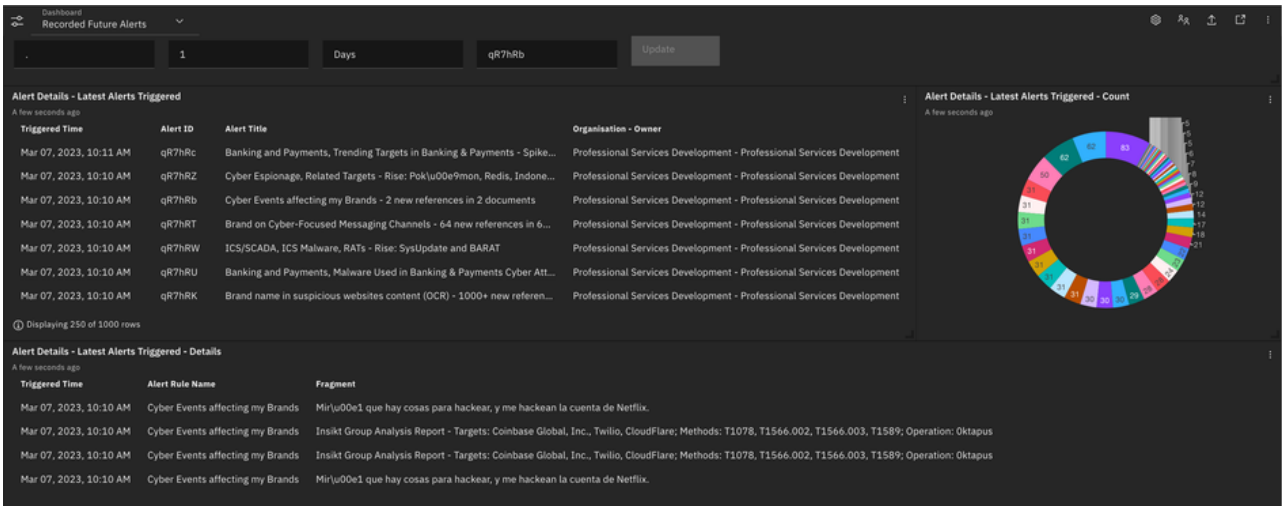
This dashboard shows the number of alerts that failed to be ingested in the `Alerts - Unknown Events` and `Playbook Alerts - Unknown Events`, the number of total alert ingested for both Legacy and Playbook and the Timeline of the ingested alerts.



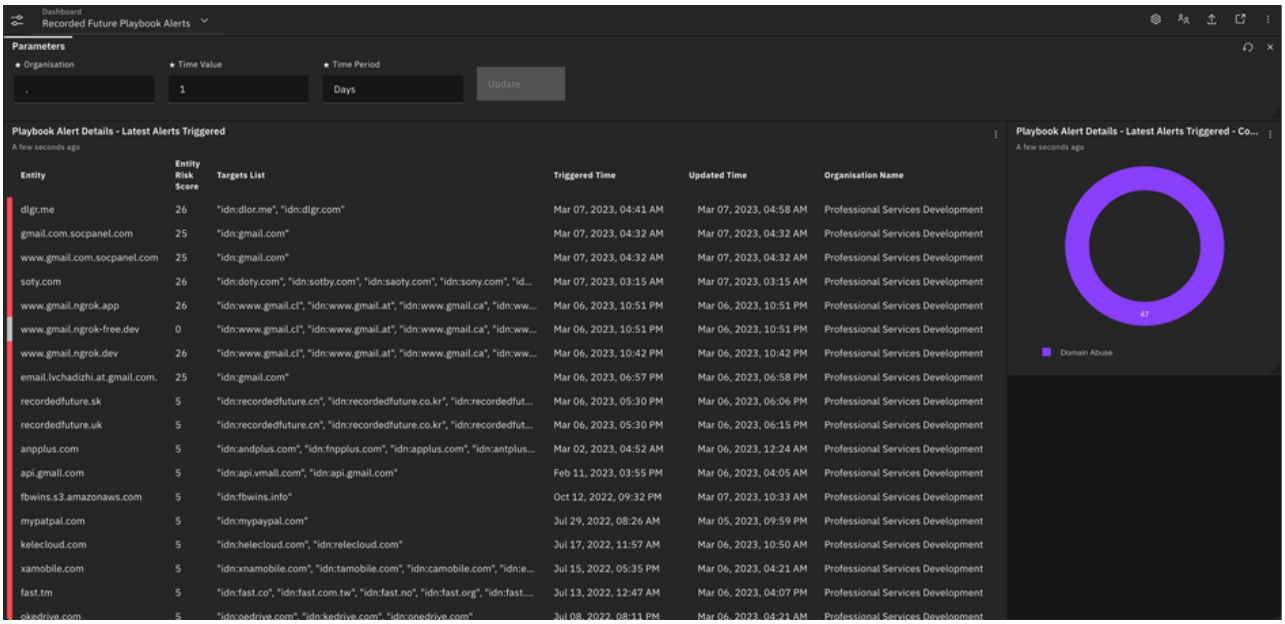
Recorded Future Alerts Statistics

Recorded Future Alerts and Recorded Future Playbook Alerts

These two dashboards show an overview of the alerts that have been parsed.



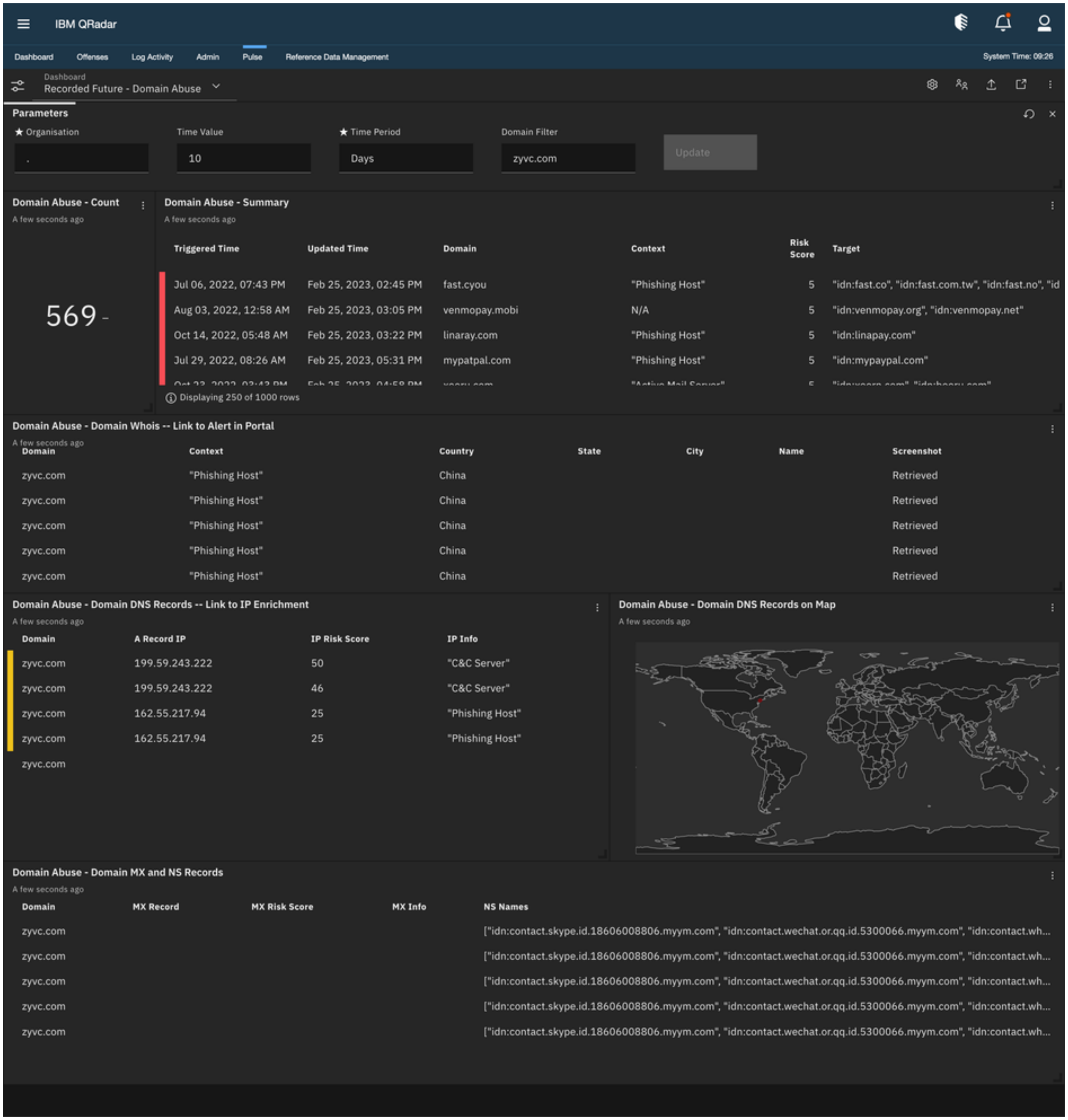
In the dashboard above, clicking on any of the alerts in the `Alert Details - Latest Alerts Triggered` will populate the widget below it (`Alert Details - Latest Alerts Triggered - Details`) with details on the specific alert.



Recorded Future - Domain Abuse

This dashboard shows the details of each domain abuse alert that has been received. Clicking on an alert in the `Domain Abuse - Summary` will populate the underlying tables with the details of the Whois data, DSN, MX and NS records.

- `Domain Abuse - Domain Whois` will redirect you to the the Recorded Future portal - a valid account is required - to view the full alert and the screenshot. The column `screenshot` will give you an idea if there is a screenshot or not with the values `Retrieved` / `Not Found`
- `Domain Abuse - Domain DNS Records` will redirect you to the enrichment of the `A Record IP`. The geolocation on the right side is provided by QRadar `GEO::LOOKUP` and it is related to the location of the IP.
- `Domain Abuse - Domain MX and NS Records` shows the details of the MX Domain and IP, along with a list of NS Names.



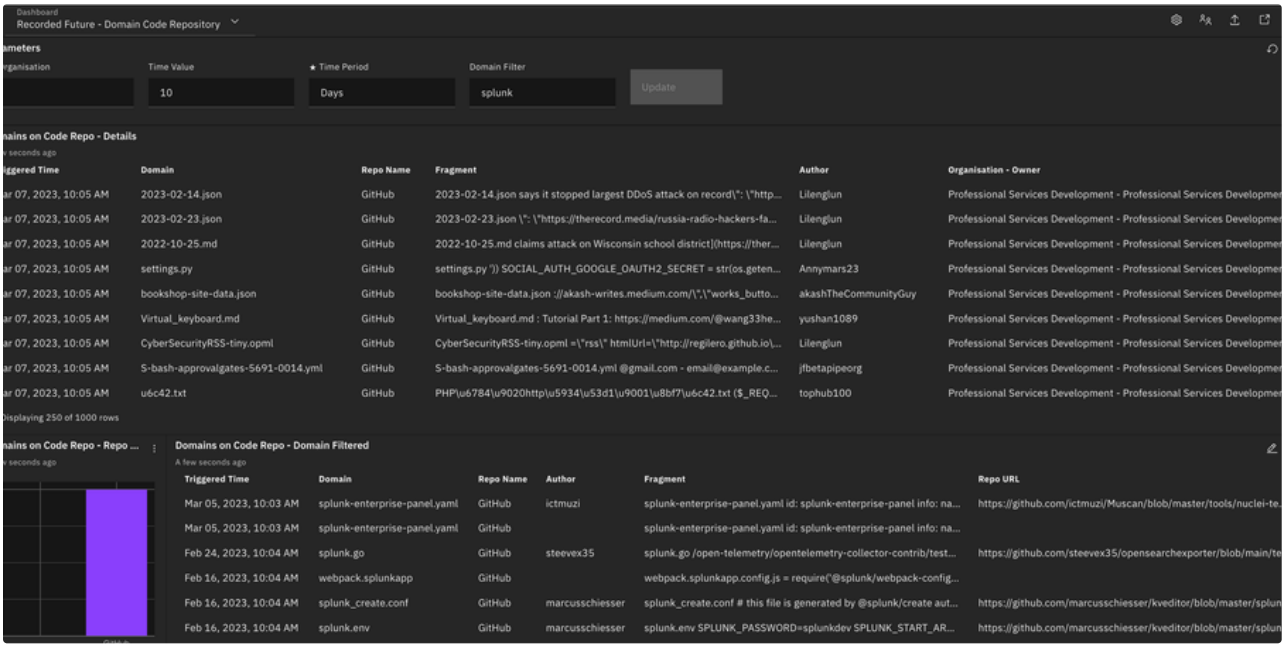
Recorded Future - Domain Abuse

Recorded Future - Domain Code Repository and Recorded Future - Email Code Repository

These two dashboards have the same layout and represent the domains and email seen in code repositories. The search filter applies for both full URLs, domains or part of the domains. In the example in the Domain Code Repository we have used `instagram` as a filter search. We could have used something more specific like `instagram.com` or `https://www.instagram.com/shannon.art_/`. The same applies for the Email Code Repository which takes part of the email, the full address or the domain.

The `Domain Filtered` and `Email Filtered` tables have been created with the idea of showing all the alerts involving a specific domain or email. Clicking on any entry in that table will redirect you to the alert in the Recorded Future Portal.

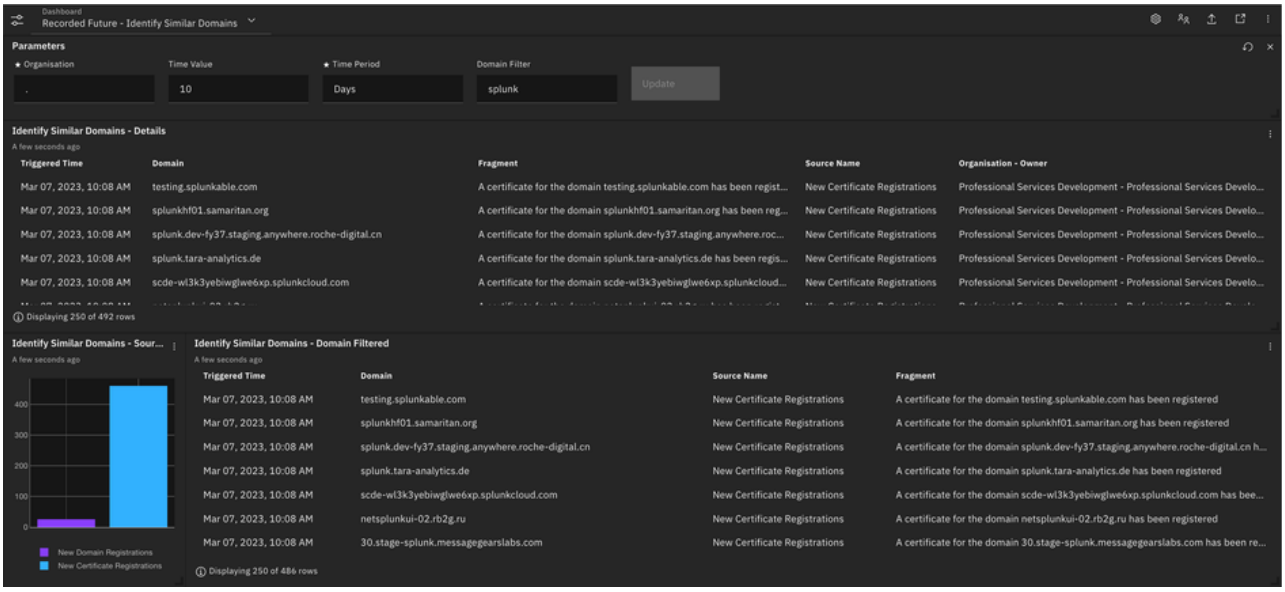
Example of Recorded Future - Domain Code Repository below:



Recorded Future - Domain Code Repository

Recorded Future - Identify Similar Domains

Similar to the above dashboards, the Identify Similar Domains shows alerts triggering from the homonym alert. The `Domain Filter` works the same as the “Recorded Future - Domain Code Repository” dashboard.

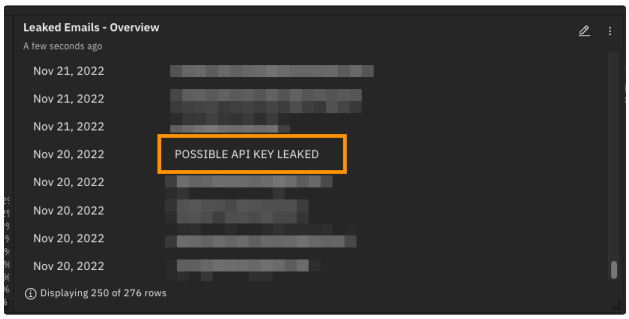


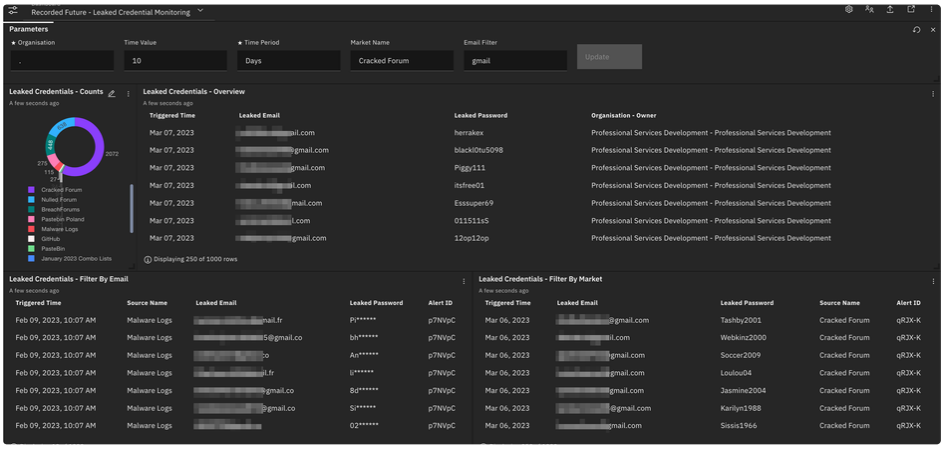
Recorded Future - Identify Similar Domains

Recorded Future - Leaked Credential Monitoring and Recorded Future - Leaked Email Monitoring

These two dashboards work in the same way as well. Both the dashboards allow to filter for Email which will populate the `Filter by Email` table (bottom) or the `Filter by Market` table on the right. Both filters allow free-text of the whole Email/Market name or part of it. In the example we have used `tesla` as a search filter. The idea is to enable you to search for all the activities in a specific Market or for a specific email address or mail domain.

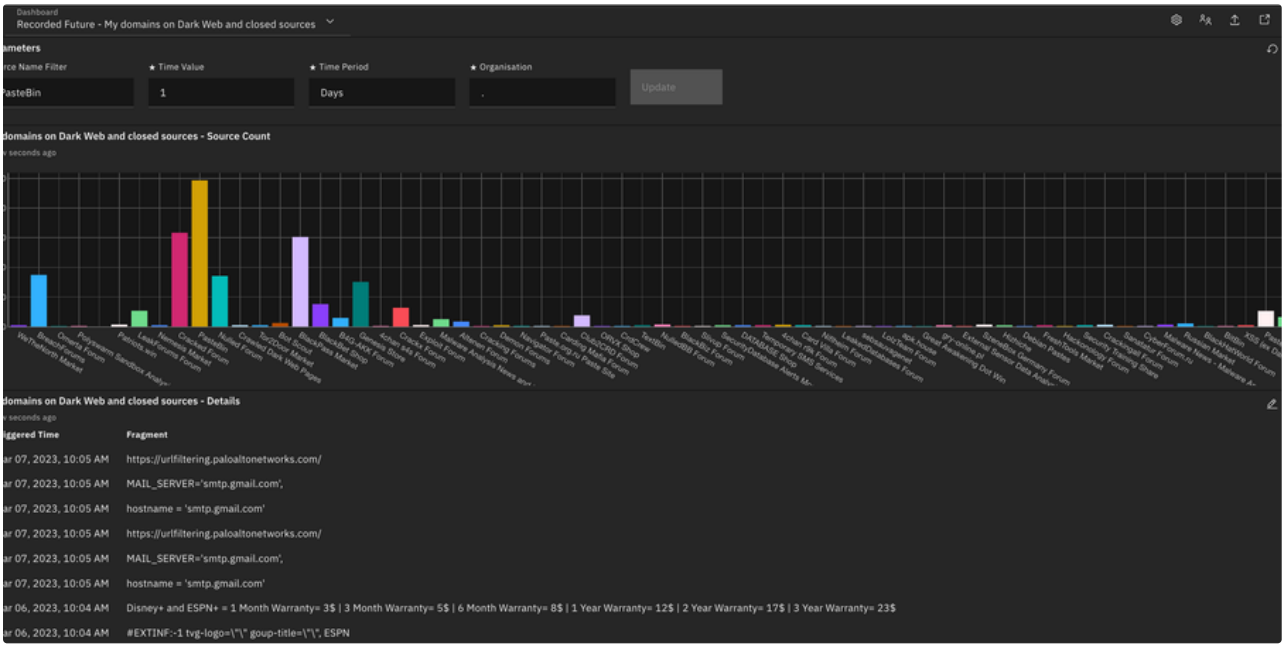
Leaked password in Leaked Email Monitoring might not be present due to the nature of the alert. There is a chance that an API Key will be captured by the alert rule. If that is the case it will be displayed with the text `POSSIBLE API KEY LEAKED` and it is required for you to log into the Recorded Future app to see the details.





Recorded Future - My domains on Dark Web and closed sources

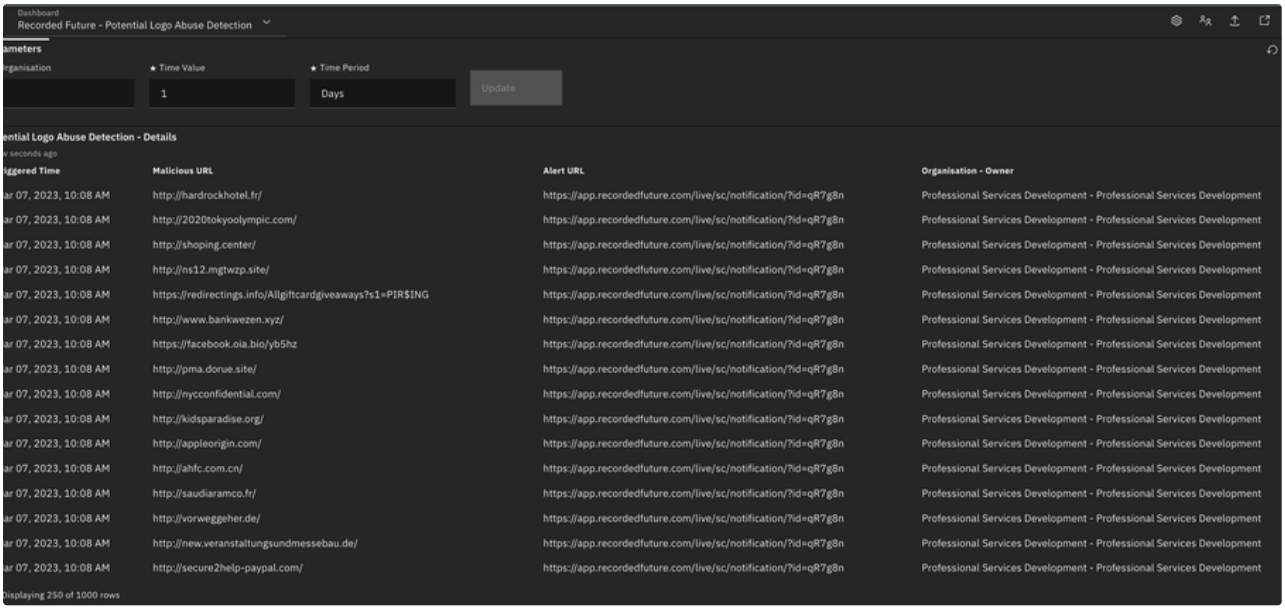
With this dashboard you will see a list of all the sources that triggers the alert with a counter of the number of alert that triggered. Clicking on each column will show the `Fragment` of the alert to give you a brief idea of what the alert is about. Clicking on the alert row itself will redirect you to the portal.



Recorded Future - My domains on Dark Web and closed sources

Recorded Future - Potential Logo Abuse Detection

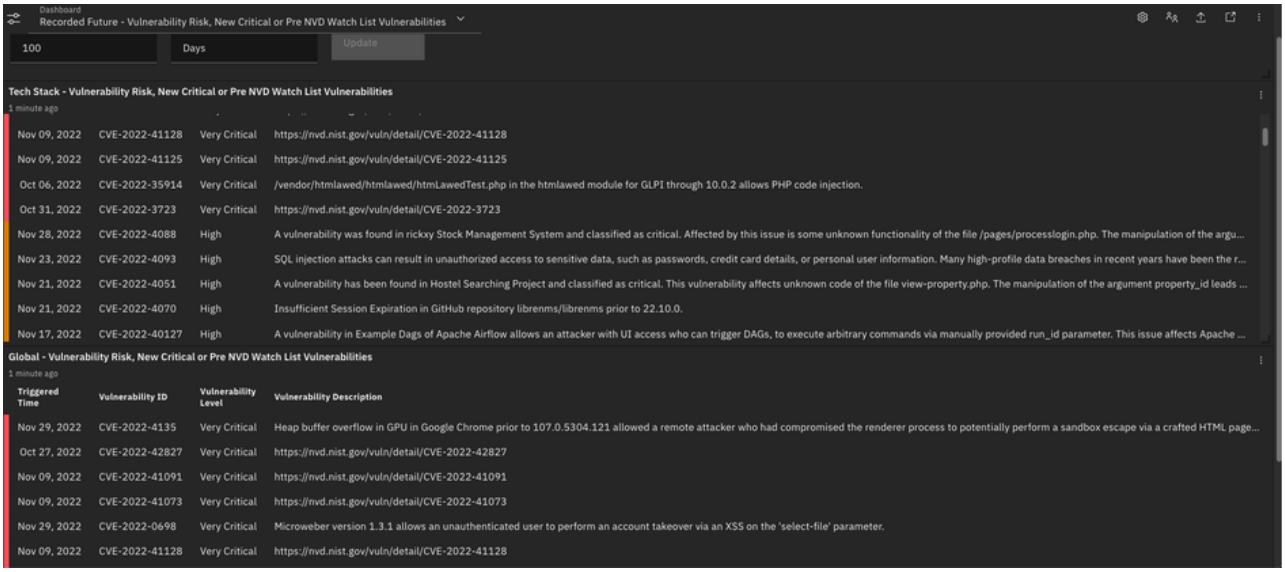
This dashboard will provide value if you have access to the Recorded Future App since clicking on any row will link you directly to the screenshot taken from page that has your company logo on it.



Recorded Future - Potential Logo Abuse Detection

Recorded Future - Vulnerability Risk, New Critical or Pre NVD Watch List Vulnerabilities

This single dashboard combines the `Tech Stack - Vulnerability Risk, New Critical or Pre NVD Watch List Vulnerabilities` and the `Global - Vulnerability Risk, New Critical or Pre NVD Watch List Vulnerabilities` alert rules, one for table. The alerts are sorted by `Criticality Level` and display the CVE that triggered the alert, the severity and a description. If the `Description` field is empty we have provided the `nvd.com` link.



Vulnerability Risk, New Critical and Pre NVD Watch List Vulnerabilities

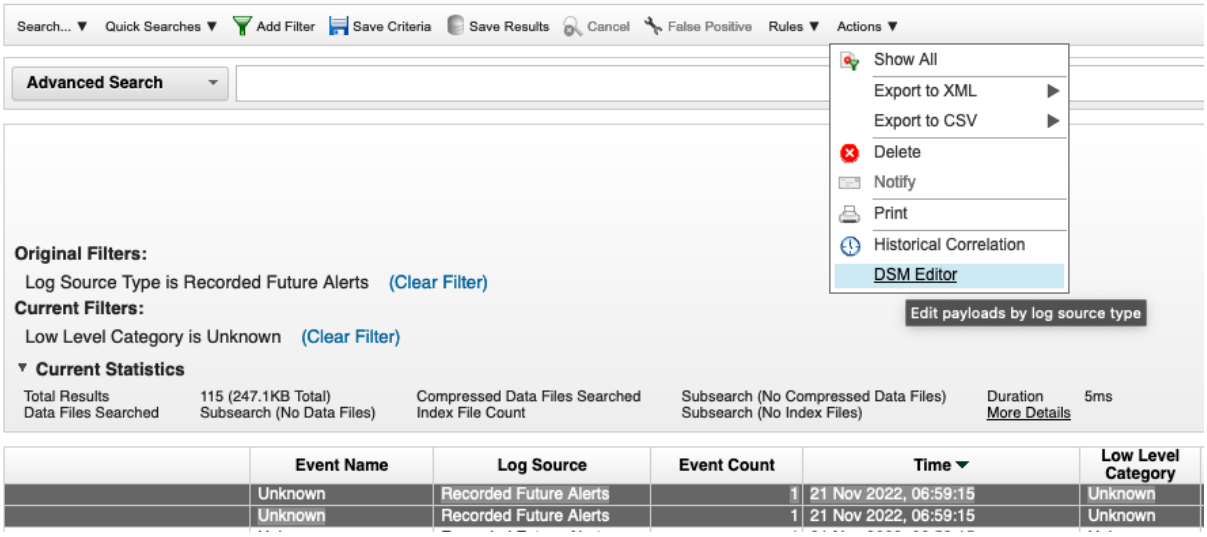
Supported Alerts

Recorded Future Intelligence Goals Library Alerts are supported and DSM mapped by default. For a complete list of supported alerts please refer to the Appendix.

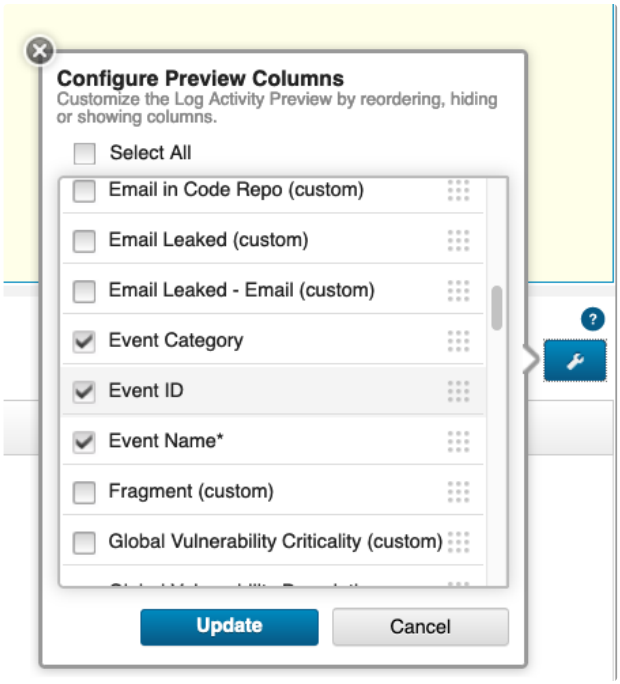
In order to parse custom alerts utilise the DSM Editor to map the custom alerts to a new QID. For more information please refer to Mapping custom alerts using the DSM Editor.

Mapping custom alerts using the DSM Editor

1. Click on the **Log Activity** tab
2. Select one or more events that are shown as **Unknown**
3. From the **Actions** list select **DSM Editor**.

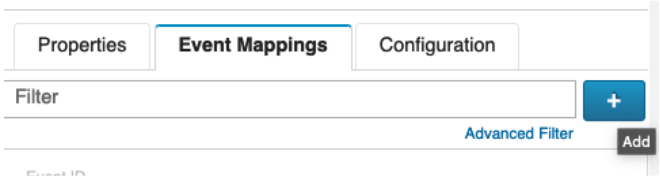


4. Click on the **Settings** icon (bottom right hand side) and select the following fields: **Event Category, Event ID, Event Name, Low Level Category**.

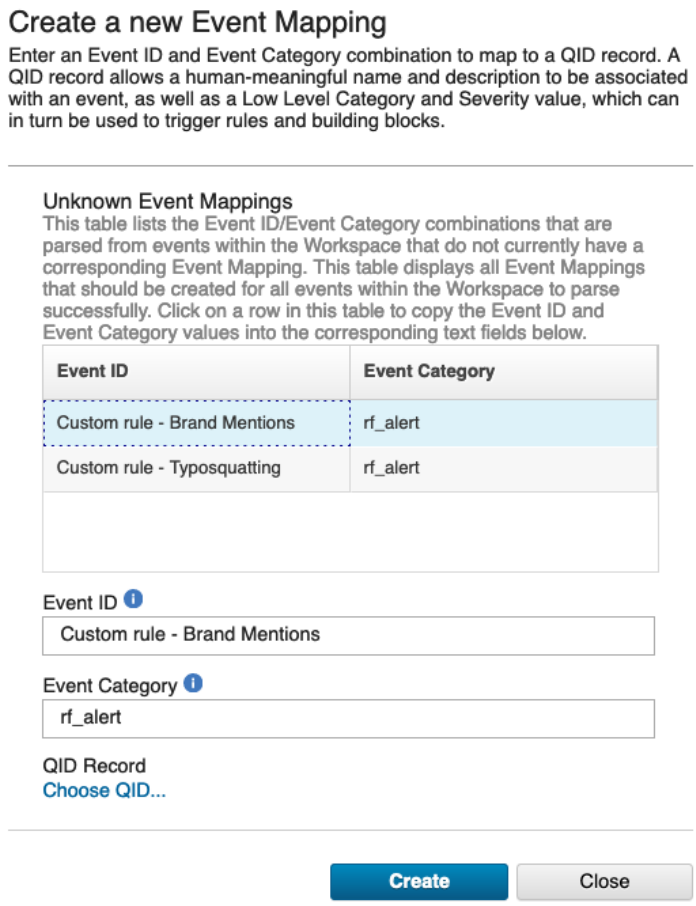


5. Review the **Log Activity (Preview)** pane. The DSM will have Event Category and Event ID extracted and ready to go as shown below:

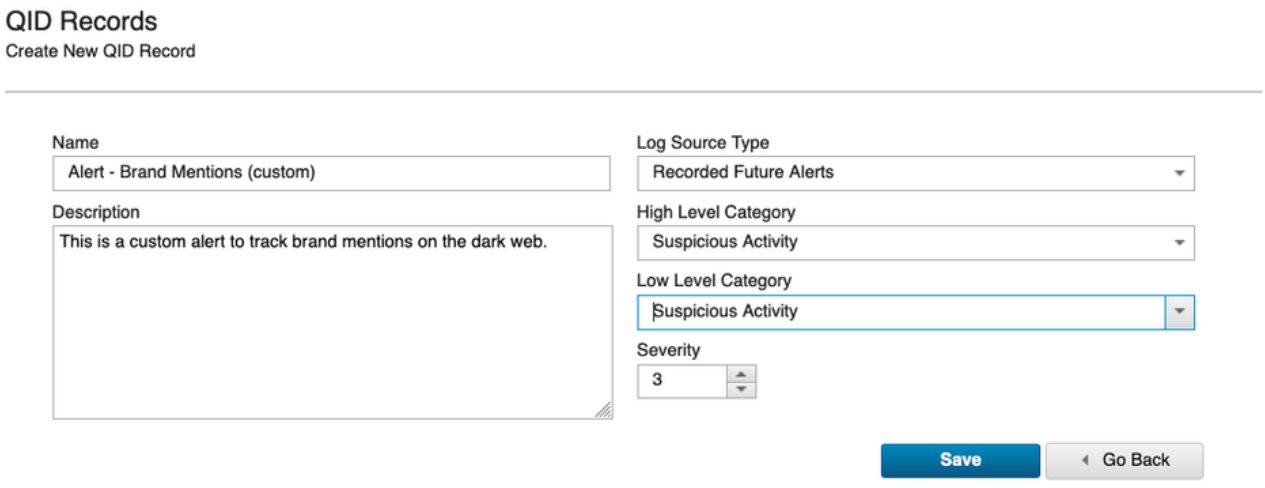
6. Click on the **Event Mappings** tab
7. Click on the blue plus icon "**+**"



8. Select the corresponding Event Category and Event ID combination, for example:



9. Click **Choose QID…**
10. Click **Create New QID Record**
11. Provide the new QID record with the necessary information, such as name, description, high and low level categories, for example:



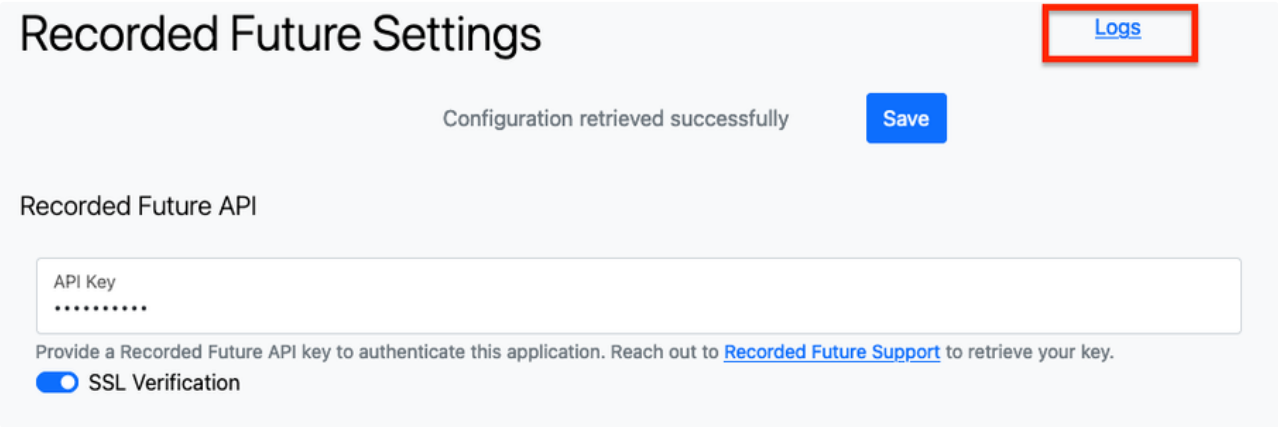
12. Click **Save**
13. Select the newly created QID and click **OK**
14. Click **Create**
15. Click **Save**

To find out more about the DSM Editor, please visit DSM Editor overview

Logging & Troubleshooting

Please refer to the following URL for instructions on how to download QRadar Application logs.
https://www.securitylearningacademy.com/course/view.php?id=4818

Additionally, application logs are available in the application configuration page.



Syslog connection issues

Verify application container can reach the syslog destination via TCP 514.

1. Connect to the backend of QRadar console / App Node
2. Open a shell inside the application container

```
/opt/qradar/support/recon connect <app id>
```

3. Send a test syslog message

```
nc -w 0 <syslog destination ip> 514 <<< "Syslog-test-message"
```

4. On the QRadar Console run a payload search for ***Syslog-test-message*** and verify the test message is found.
5. If the the above steps fail, then verify network routing and firewall settings.

Logs indicate alerts were sent to QRadar, but search returns no alerts

After alert events have been sent to QRadar via Syslog the Event Pipeline in QRadar needs to process and store those events, this cane take several minutes. Meaning that a search might not find the events that have been ingested a minute ago. Wait for a few minutes and try again.

Truncation of events

Not all Recorded Future alerts are equal and some are rather large and might get truncated by the QRadar event pipeline. Try increasing the **Max TCP Syslog Payload Length** from 12K to a larger value, but please do so careful and involve IBM QRadar Support if needed as increasing the size can have a negative impact on the performance of QRadar.
To increase the **Max TCP Syslog Payload Length**, click here.

Reference: QRadar: TCP and UDP Syslog Maximum Payload Message Length for QRadar Appliances

Not fetching alerts

The integration only fetches alerts with a status of `no-action` or as shown in the portal `New`. Verify that the alerts you wish to fetch have this status set.

Appendix

Supported Alert Rules

- Analyst-On-Demand Report
- Banking and Payments, Attackers in Banking & Payments Cyber Attacks
- Banking and Payments, Malware Used in Banking & Payments Cyber Attacks
- Banking and Payments, Banking Trojans, ATM Malware, Exploit Kits Malware
- Banking and Payments, Trending Targets in Banking & Payments
- Banking and Payments, Vulnerabilities Recently Related to Banking & Payments
- Brand name in suspicious websites content (OCR)
- Brand on Cyber-Focused Messaging Channels
- Brand Mentions with Cyber entities
- Company Email on Code Repository
- Credit Card Monitoring
- Cyber Espionage, RATs, Exploits, and Rootkits
- Cyber Espionage, Related Targets
- Cyber Espionage, Related Vulnerabilities
- Cyber Espionage, APT Threat Actors
- Cyber Events affecting my Brands
- Domains on Code Repositories
- Executive Impersonation on Social Media
- Executive Impersonation on professional networking website
- Exploit Kit Modification
- Gift Card Monitoring
- Global Third-Party Risk, Risk
- Global Third-Party Risk, Trend
- Global Trends, Trending Attackers
- Global Trends, Trending Operations
- Global Trends, Trending Vulnerabilities
- Global Trends, Trending Methods
- Global Trends, Trending Targets
- Global Vulnerability Risk, New Critical or Pre NVD Vulnerabilities
- Global Vulnerability Risk, Vendors and Products Mentioned with Vulnerabilities
- Global Vulnerability Risk, Vulnerabilities Recently Linked to Malware
- Global Vulnerability Risk, Vulnerabilities Recently Linked to Pentest Tools
- Global Vulnerability Risk, Vulnerabilities, New Exploit Chatter
- ICS/SCADA, ICS Malware, RATs
- ICS/SCADA, Trending Targets in ICS/SCADA
- ICS/SCADA, Vulnerabilities Related to ICS/SCADA Cyber Attacks
- ICS/SCADA, Attackers in ICS/SCADA Cyber Attacks

- ICS/SCADA, Malware Used in ICS/SCADA Cyber Attacks
- IP Address Mentions
- Identify Similar Domains
- Increased Domain Risk Score
- Increased IP Address Risk Score
- Industry Risk, Trending Attackers in Industry
- Industry Risk, Trending Companies in Industry
- Industry Risk, Trending Industry Peers in Watch List
- Industry Risk, Trending Methods in Industry
- Infrastructure and Brand Risk, Brand Names in Watch Lists
- Infrastructure and Brand Risk, Potential Typosquatting Watch List Domains
- Leaked Credential Monitoring
- Leaked Email Monitoring
- Mentions of Service Disruptions
- My brands on Dark Web and closed sources
- My domains on Dark Web and closed sources
- Phishing or Spam Campaigns (Phishing Related to Operations)
- Possible Fake Apps Detection
- Potential Logo Abuse Detection
- Ransomware, Software Recently Linked to Ransomware
- Ransomware, Vulnerabilities Recently Linked to Ransomware
- Target Trends, Trending Attackers Linked to Targets
- Target Trends, Trending Methods Linked to Targets
- Target Trends, Trending Operations Linked to Targets
- Target Trends, Trending Related Attackers
- Target Trends, Trending Targets in Watch List
- Third-Party Risk, Risk
- Third-Party Risk, Trend
- Trends, Trending Operations in Watch List
- Trends, Trending Watch List Attackers
- Trends, Trending Watch List Methods
- Trends, Trending Watch List Operations
- Trends, Trending Watch List Targets
- Trends, Trending Watch List Vulnerabilities
- Vulnerability Risk, Watch List Vendors & Products Mentioned with Vulnerabilities
- Vulnerability Risk, New Critical or Pre NVD Watch List Vulnerabilities
- Vulnerability Risk, Watch List Vulnerabilities Linked to Pentest Tools
- Vulnerability Risk, Watch List Vulnerabilities New Exploit Chatter
- Vulnerability Risk, Watch List Vulnerabilities Recently Linked to Malware
- Vulnerability Risk, Watch List Vulnerabilities with Proof of Concept code available

Out-of-the-box Custom Event Properties (CEP)

- Alert Category
- Alert ID

- Alert Priority
- Alert Rule Name
- Alert Seq
- Alert Seq Total
- Alert Source Name
- Alert Title
- Alert Triggered Time
- Alert URL
- Alert Updated Time
- DNS - A Record IP
- DNS - A Record IP Info
- DNS - A Record IP Risk Score
- DNS - NS
- Domain Abuse Context
- Domain Code Repo
- Email Leaked
- Email Leaked - Email
- Email in Code Repo
- Entity Criticality
- Entity Subject
- Entity Risk Score
- Fragment
- Global Vulnerability Criticality
- Global Vulnerability Description
- Global Vulnerability ID
- Global Vulnerability Level
- Global Vulnerability Source URL
- Latest Screenshot
- Leaked Password
- Logo ID
- Logo URL
- MX - Domain
- MX - Domain Info
- MX - Domain Risk Score
- Owner Name
- Repo Source Author
- Repo URL
- RF Organisation
- Similar Domain
- Status In Portal
- Targets List
- Whois - City
- Whois - Country
- Whois - Name
- Whois - State